NOAA CIO Council
Meeting Minutes
March 7, 2003

Attendees:

Carl Staton, Chair
Bill Turnbull
Greg Bass
Nancy Huang
Hugh Johnson
Rob Mairs
Larry Tyminski
Barry West
Sandy Wine
Charles MacFarland
Gerald Singleton
Bill Martin
Ron Trenti
John D. Parker
Mike Hart
Rebecca Vasvary
Conrad Lovely
Diane Davidowicz
Jeremy Warren
Joe Smith
Rick Roberts

Purpose: This was a special meeting held to discuss an expected Departmental Call for 24/7 Emergency Notification Procedures for Alerts. Operating Units need to prepare procedures to inform CIOs/ITSOs/System Administrators about the need for immediate patches and other actions. The expected due date is 3/12.

Decisions:

A chart of the following process is attached to these minutes.

Initial Contacts - The Department will require at least two points of initial contact in an Operating Unit, with alternates. For NOAA these will be the NOAA CIO/Deputy CIO, the Director of the IT Security Office/NOAA IT Security Officer, and the NOAA CIRT.

First-Level Action - The NOAA CIRT and the NOAA Security Officer will coordinate on an immediate technical analysis and an analysis of possible actions. The NCIO will analyze the external factors involved with the problem. If specific action has been directed by the Department, the NCIO will negotiate with the Department if the action time appears unreasonable. The NCIRT, the NOAA IT Security Office, and NCIO will determine the final action decision. That will be distributed by the NCIRT. The method of contact, either phone or e-mail or both, depends on the type of action involved.

Actions will fall into one of three groupings: Notices, Watches, and Warnings.

> Notices are general possible problems where there is no action time assigned and L.O.s can take action as they determine it is needed, perhaps during the next scheduled patch process.
>
> Watches are situations where there is a more immediate potential threat to NOAA systems, but the neither the Department or first-level NOAA decision-makers consider it necessary to assign a general action time. Individual L.O.s may decide that their specific situations require immediate action, that it can wait until normal working hours, etc., depending on the local threat.
>
> Warnings are situations where NOAA systems are already compromised or the threat is considered so great that either the Department or the first-line decision-makers decide that action must be taken within a certain time.

Second-Level Action - The decision taken at the first level will be transmitted to the ITSOs. General Notices will be handled as in the past. Watches will be handled as determined by the L.O., with the timing and degree of coordination between the ITSO and L.O. CIO determined by their procedures. Warning will require the ITSO to activate the 24/7 notification tree. The NCIO may contact the L.O. CIOs if specific actions/times are directed from above.

Third -Level Action - System Administrators will be notified by the ITSOs. For Warnings they must be available 24/7 by either cell phone or pager, although we do not need to provide them with these immediately. For Notices or Watches e-mails or phone contact may be used, depending on the situation within the Line Office. ITSOs will need to have their notification lists available at all times.

Feedback - We anticipate that Warnings will usually entail some feedback mechanism on the actions taken. The instructions for specific incidents will detail what information will need to be provided and how. Feedback will usually be to the NCIO and Deputy NCIO, the CIRT, and the Director of the IT Security Office/NOAA IT Security Officer. E-mail will normally be used for feedback.

Personnel Issues: In addition to the normal concerns about the impact on resources, there were also concerns about how current contracts and employee rules will allow the type of 24/7 actions that may be required. These problems will have to be addressed.

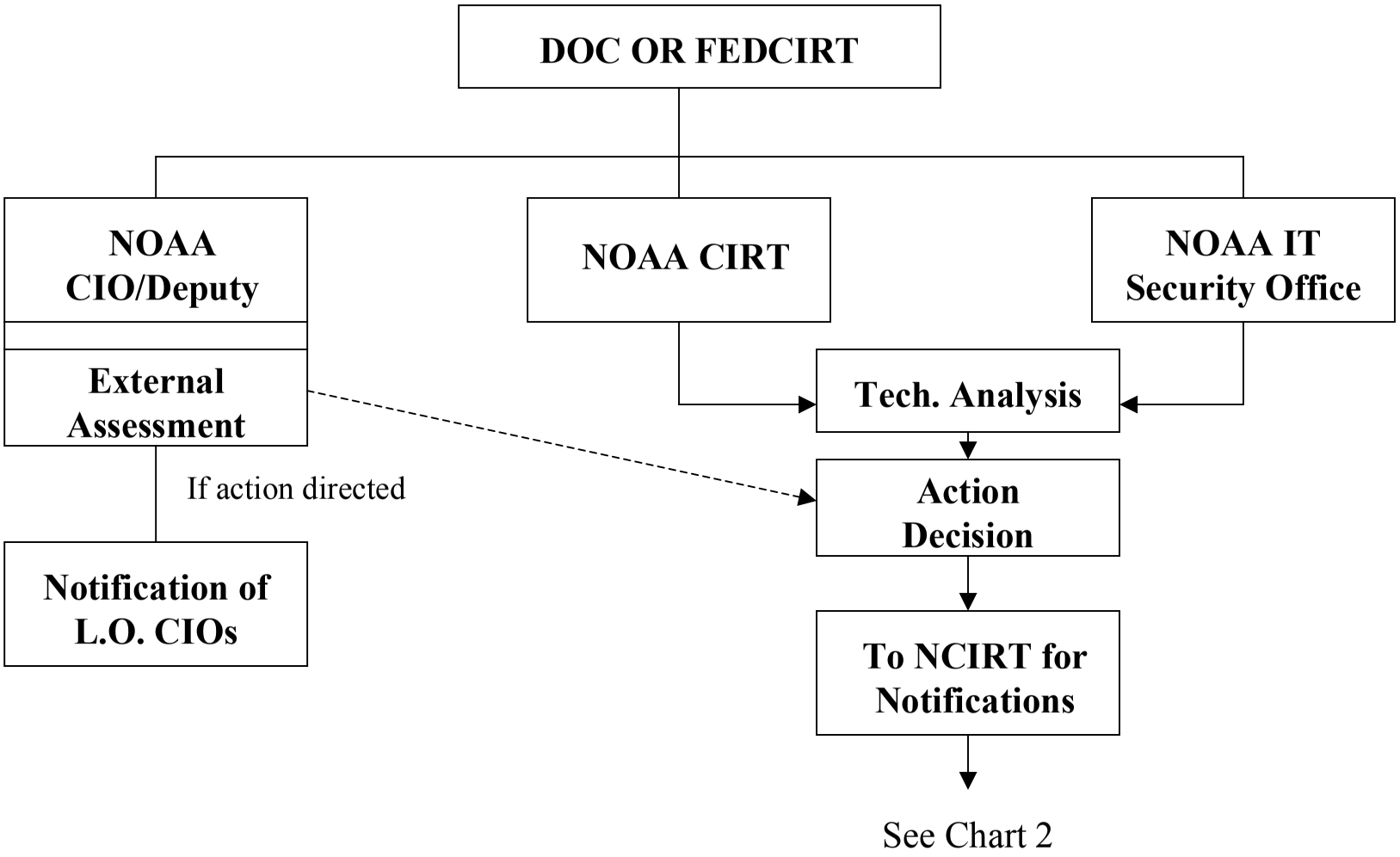
Actions Required: L.O. CIOs need to provide Carl with a Notification Tree before the 12th. The tree must include the CIOs and ITSOs, of course, but also go down to all System Administrators, not just those for major systems.

The list must include the following: name, phone numbers at home and office, cell phone and/or pager, and e-mail address. If no cell phone or pager number is available at this point, indicate

that. For cell phones/pagers indicate whether text messaging can be used (with address if available).

The NOAA Notification Tree will be placed in a binder and shown to Tom Pyke.

NOTIFICATION PROCEDURES (1)



NOTIFICATION PROCEDURES (2)